IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA	
v.	CRIMINAL CASE NO. 1:14-CR-00227-TCB-RGV
DAVID LEE, *et al.*	

MAGISTRATE JUDGE'S REPORT, RECOMMENDATION, AND ORDER ON DEFENDANT'S PRETRIAL MOTIONS

Defendant David Lee ("Lee") is charged with conspiring to infringe copyrights and to circumvent a technological measure that effectively controls access to a copyrighted work, in violation of 18 U.S.C. § 371, and aiding and abetting criminal copyright infringement, in violation of 17 U.S.C. § 506(a)(1)(A) and 18 U.S.C. §§ 2 and 2319(b)(1). [Doc. 1].[1] Lee has filed a "Motion to Require the Government to Remove Portions of an Offending Press Release from All DOJ Websites," [Doc. 53],[2] and a "Motion to Suppress Evidence Seized Pursuant to Two

[1] The listed document and page numbers in citations to the record refer to the document and page numbers shown on the Adobe file reader linked to the Court's electronic filing database, CM/ECF, except that citations to the evidentiary hearing transcript are cited according to the transcript page number.

[2] The government has filed a response opposing Lee's motion, [Doc. 53], to which Lee has filed a reply, [Doc. 61].

Constitutionally Deficient Warrants," [Doc. 54].[3] Following an evidentiary hearing held on February 26, 2015,[4] Lee filed a supplemental brief in support of his preliminary motion to suppress evidence, [Doc. 68], and the government filed a response to Lee's motion to suppress evidence, [Doc. 71].[5] For the reasons that follow, Lee's "Motion to Require the Government to Remove Portions of an

[3] On January 8, 2015, Lee also filed a motion to suppress statements, [Doc. 52], but that motion has been deferred to the District Judge, [Doc. 63].

[4] See [Doc. 66] for the transcript of the evidentiary hearing. Citations to the evidentiary hearing transcript hereinafter will be referred to as "(Tr. at ___)." Lee elected to waive his right to attend the evidentiary hearing. [Doc. 62]; (Tr. at 3–4).

[5] Lee subsequently filed a reply to the government's response, [Doc. 78], and on June 5, 2015, the government filed a motion for leave to file a surreply, [Doc. 80], to Lee's reply brief regarding the motion to suppress evidence. Although "[n]either the Federal Rules nor the Court's Local Rules allow sur-reply briefs as a matter of right, and the Court normally does not permit sur-replies," USMoney Source, Inc . v. Am. Int'l Specialty Lines Ins. Co., No. 1:07-cv-0682-WSD, 2008 WL 160709, at *2 n.5 (N.D. Ga. Jan. 15, 2008), rev'd on other grounds, 288 F. App'x 558 (11th Cir. 2008) (per curiam) (unpublished) (citation omitted), "the Court may in its discretion permit the filing of a surreply . . . where a valid reason for such additional briefing exists, such as where the movant raises new arguments in its reply brief," Fedrick v. Mercedes-Benz USA, LLC, 366 F. Supp. 2d 1190, 1997 (N.D. Ga. 2005) (citations omitted). Here, the government seeks leave to file a surreply to address a particular argument raised by Lee for the first time in his reply brief. See [Doc. 80 (seeking to address Lee's argument that a certain representation made by the government in its responsive brief is inconsistent with the evidence of record and the prosecutor's prior representations to the Court)]. Accordingly, for good cause shown, the government's motion for leave to file a surreply, [id.], is **GRANTED**, and the Clerk is **DIRECTED** to enter the government's surreply, [Doc. 80-1], on the docket.

Offending Press Release from All DOJ Websites," [Doc. 53], is **DENIED**, and it is **RECOMMENDED** that Lee's motion to suppress evidence, [Doc. 54], be **DENIED**.

I. STATEMENT OF FACTS

On November 8, 2011, the Federal Bureau of Investigation ("FBI") obtained search warrants for two email accounts, "thebuzzer@gmail.com" and "flyingbuzz@gmail.com," both of which were connected to "www.applanet.net," a website that was allegedly involved in the illegal distribution of copyrighted works. [Doc. 54-1]. Each of the warrants included attachments describing the information that Google was required to disclose pertaining to the email accounts, [id. at 20–22, 46–48], and identifying which items of information from within the required disclosure would be subject to seizure by the government, [id. at 23, 49]. In particular, Attachment A on each warrant describes the "Items to be Disclosed by the Provider," and lists five categories of requested information as specified in paragraphs A through E; while Attachment B, which lists the "Items to be Seized" by the government, is comprised of two categories of information that would be subject to seizure as identified in paragraphs A and B of that attachment. [Id. at 20–23, 46–49]. Paragraphs A and B of Attachment A required Google to disclose the contents of any electronic communications or files belonging to the relevant account; paragraph C required disclosure of any Gmail IDs listed on the subscriber's Friends

list; paragraph D required disclosure of basic subscriber information, such as name, telephone, physical address, and Internet Protocol ("IP") address information; and paragraph E required disclosure of user connection log information related to each account. [Id. at 20–22, 46–48]. Taken together, paragraphs A through E of Attachment A essentially directed Google to disclose all of the contents of the Gmail accounts in question. See [id.]; (Tr. at 16, 19–20). As for Attachment B of the warrants, paragraph A identifies evidence of copyright infringement—specifically, evidence of violations of 17 U.S.C. § 506 and 18 U.S.C. § 2319—as the items to be seized by the government upon its receipt of the information described in Attachment A. [Doc. 54-1 at 23, 49]. Paragraph B of Attachment B further identifies the information specified in paragraphs C through E of Attachment A as being subject to seizure. [Id.].[6]

[6] Similarly, each of the search warrant affidavits requested that Google be required to disclose to the government the records and information particularly described in Attachment A, and provided that, "[u]pon receipt of the information described in Attachment A, the information described in Attachment B, which includes any evidence, fruits, and instrumentalities of violations of 17 U.S.C. § 506 and 18 U.S.C. § 2319 (infringement of a copyright), will be subject to seizure by law enforcement." [Doc. 54-1 at 13, 39]. See also [id. at 13–14, 39–40 (search warrant affidavits requesting "that the Court issue a search warrant directed to Gmail requiring it to disclose to the government the information described in Attachment A and thereafter authorizing the government to seize the information described in Attachment B")].

At the evidentiary hearing held on February 26, 2015, FBI Special Agent Kevin Orkin ("Agent Orkin"), testified that he had executed the search warrants for Lee's Gmail accounts and received the required production from Google in response to the search warrants. (Tr. at 7). Agent Orkin explained that, upon his receipt of a response to a search warrant for an online account, he would typically begin by copying the response onto a laptop and then loading the response into an email-reading client for analysis. (Id.). Next, he would "start the triage, or the analysis of the email," which usually consisted of keyword searches, "sorting by the recipient or sender," or identifying certain companies, such as PayPal, that he "knew were used in an investigation[.]" (Tr. at 8). He would then organize the targeted information into "subfolders that [he] created so that [he] could go back and read through them." (Id.).

Agent Orkin did not recall whether he actually used keyword searches to analyze Google's production with respect to Lee's Gmail accounts in particular, although he did recall "triaging [the production] for relevancy to the investigation." (Tr. at 18, 21–22); see also (Tr. at 22 (testifying that he "went through the e-mails and determined if they related to this investigation or the affidavit")). He also selected certain emails from Lee's Gmail accounts that "were of importance in the investigation for creating additional leads," e.g., "for additional search warrants or

to prepare other agents to conduct interviews in the investigation." (Tr. at 8–9); see also (Tr. at 19). When asked what he did with the emails he had selected, Agent Orkin responded that he included "some of the emails . . . in leads to the offices that were going to be executing knock and talks and search warrants," in order to better prepare agents who had no prior knowledge of the investigation. (Tr. at 9).[7] Although Agent Orkin acknowledged that Google's production included emails that were not related to the investigation, he did not segregate those emails from those that were related to the investigation, nor did he make a list identifying which emails were subject to seizure according to the parameters set forth in Attachment B of the warrants. (Tr. at 22–23); see also (Tr. at 23 (testifying that "[t]he emails that are not related to the investigation are still contained in the response that Google provided")).[8]

Agent Orkin further testified that, before the search warrants for Lee's Gmail accounts were obtained or executed, he knew that the accounts had originally been opened in 2004. (Tr. at 12–13, 16). Additionally, at the time he executed the

[7] Agent Orkin also confirmed that he could recreate his selections of the emails "without resorting to going back to the original evidence[.]" (Tr. at 9).

[8] The government turned over Google's entire production to Lee in discovery. (Tr. at 23–24).

warrants, he knew that Applanet did not exist in its present form in 2004, but he did not know whether it existed "in any form" in 2004. (Tr. at 17).

II. DISCUSSION

A. Lee's "Motion to Require the Government to Remove Portions of an Offending Press Release from All DOJ Websites," [Doc. 53]

Following Lee's indictment, the Department of Justice ("DOJ") issued a press release describing the charges against Lee and other individuals charged with similar offenses related to copyright infringement. See [Doc. 53 at 11–12 (press release)]. The press release includes quotes from DOJ officials stating that "these defendants are now being held accountable for the intellectual property they stole," and that "[a]s a result of their criminal efforts to make money by ripping off the hard work and creativity of high-tech innovators, the defendants are charged with illegally distributing copyrighted apps[.]" [Id. at 11]. Lee argues that these statements violate both the DOJ's own regulations and this Court's Local Rules concerning the release of information in criminal cases. See generally [Doc. 53]. In particular, Lee asserts that the statements violate 28 C.F.R. § 50.2 and Criminal Local Rule 57.4A.

The DOJ's statement of policy on the disclosure of information by DOJ personnel relating to criminal and civil proceedings is set forth at 28 C.F.R. § 50.2. The statement includes a series of "generally applicable guidelines," 28 C.F.R. §

50.2(b)(9), that are intended to "strik[e] a fair balance between the protection of individuals accused of crime," and "public understandings of the problems of controlling crime and administering government," 28 C.F.R. § 50.2(a)(2). The guidelines provide that disclosures in criminal cases "should include only incontrovertible, factual matters, and should not include subjective observations," 28 C.F.R. § 50.2(b)(3), and also that the DOJ "should refrain" from disclosing "[o]bservations about a defendant's character," "[s]tatements concerning evidence or argument in the case," or "[a]ny opinion as to the accused's guilt," 28 C.F.R. § 50.2(6)(i), (v), and (vi).

The statements about which Lee complains in this case do not appear to run afoul of the DOJ's guidelines, as the statements are essentially a factual description of the substance of the charges on which he has been indicted, and they offer no opinion as to Lee's character or alleged guilt, or as to any "evidence or argument" in the case. In any event, Lee cannot obtain the relief he seeks under 28 C.F.R. § 50.2 since that regulation "does not create a private right of action," United States v. Howard, Criminal Action No. 12–1, 2014 WL 2429315, at *3 n.2 (E.D. La. May 29, 2014) (citation omitted), and Lee therefore lacks standing to enforce it, see Harris v. Holder, 885 F. Supp. 2d 390, 401 (D.D.C. 2012) (citation omitted) (finding plaintiff entitled to no relief based on alleged violations of 28 C.F.R. § 50.2 since "there is no

private right of action under this regulation"); Hatfill v. Ashcroft, 404 F. Supp. 2d 104, 121 (D.D.C. 2005) ("[28 C.F.R. § 50.2] is a policy statement promulgated by the DOJ . . . . Absent a clear indication of congressional intent to create a private right of action for the enforcement of this regulation, the Court can not impose one.").

Along the same lines, Criminal Local Rule 57.4A addresses the release of information in criminal proceedings by lawyers or law firms:

> From the time of arrest[] . . . or indictment . . . until the commencement of trial or disposition without trial, a lawyer or law firm associated with the prosecution or defense shall not release . . . any extrajudicial statement . . . relating to that matter and concerning . . . the character or reputation of the accused, . . . [a]ny opinion as to the accused's guilt or innocence or as to the merits of the case or the evidence in the case.

LCrR 57.4A(3)(a) and (f), NDGa. As previously mentioned, the statements about which Lee complains say nothing about Lee's character or reputation, nor do they espouse an opinion as to Lee's guilt or innocence, or as to the merits or evidence of the government's case against him. To the contrary, the DOJ's press release announcing Lee's indictment explicitly states that the "[c]harges contained in an indictment are merely allegations, and the defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law." [Doc. 53 at 12].

In addition, Rule 57.4A cautions that it "shall not be construed to preclude the lawyer or law firm . . ., in the proper discharge of official or professional obligations,

from . . . disclosing the nature, substance, or text of the charge, including a brief description of the offense charged[.]" LCrR 57.4A(3), NDGa. By issuing the press release in this case, the DOJ disclosed a series of indictments pertaining to the alleged copyright infringement of recent and widely popular technological innovations, and thereby properly discharged its responsibility of "making available to the public information about the administration of the law" on a matter of significant public interest. See 28 C.F.R. § 50.2(a)(2) (noting that "there are valid reasons for making available to the public information about the administration of the law"). Nor was the DOJ's disclosure any less proper simply because the description of the nature and substance of the charges contained in the indictments was conveyed in ordinary language, rather than in the technical legal terms of the indictments. Compare [Doc. 1 at 17 ¶ 5 (indictment charging Lee with, among other offenses, "aid[ing] and abett[ing] others, who willfully and for the purposes of private financial gain did infringe copyrights by reproducing and distributing during a one hundred eighty (180) day period ten (10) or more copies of one (1) or more copyrighted works, namely copyrighted mobile device software applications (or "apps"), with a total retail value of more than $2,500," "[a]ll in violation of Title 17, United States Code, Section 506(a)(1)(A) . . . .")], with [Doc. 53 at 11 (describing the charges of copyright infringement as "criminal efforts" to "rip[] off" the "hard

work and creativity of hi-tech innovators," and explaining that the defendants who have been indicted are now "being held accountable for the intellectual property they stole" as charged in the indictment)].[9] Accordingly, Lee's "Motion to Require the Government to Remove Portions of an Offending Press Release from All DOJ Websites," [Doc. 53], is **DENIED**.

B. Lee's Motion to Suppress Evidence, [Doc. 54]

Lee argues that any evidence seized pursuant to the search warrants in this case should be suppressed because: (1) the warrants are general warrants that do not satisfy the Fourth Amendment's particularity requirement, [Doc. 54 at 7–14; Doc. 68 at 3–6]; (2) the warrants were executed in a constitutionally flawed manner, [Doc. 54 at 14–17; Doc. 78 at 12–15]; and (3) the warrants were obtained by omitting material facts in violation of Franks v. Delaware, 438 U.S. 154 (1978), [Doc. 68 at 6–8; Doc. 78 at 11–12]. The Court will address each of Lee's arguments in turn.

1. The Warrants Satisfy the Particularity Requirement

Lee argues that the warrants used to seize his Gmail accounts are general warrants that do not satisfy the Fourth Amendment's particularity requirement, since they required unlimited disclosure of "all of the information [Google]

[9] The parties also dispute the particular legal basis on which the Court could grant Lee the relief he seeks pursuant to Criminal Local Rule 57.4. See [Doc. 60 at 4 & n.1, 6–9; Doc. 61 at 6–8]. Since the Court finds that the challenged statements did not violate this rule, there is no need for the Court to address these arguments.

possessed" relating to Lee's email accounts. [Doc. 54 at 7–14; Doc. 68 at 3–6]. The government responds that the warrants satisfied the particularity requirement because they appropriately limited the information to be seized by law enforcement according to certain specific categories of information related to the criminal activity under investigation. [Doc. 71 at 6–13].

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. See also Fed. R. Crim P. 41. "The 'manifest purpose' of the 'particularity requirement of the Fourth Amendment' is 'to prevent general searches.'" United States v. Ellis, 971 F.2d 701, 703 (11th Cir. 1992) (quoting United States v. Leon, 468 U.S. 897, 963 (1984) (Stevens, J., concurring)). "A general order to explore and rummage through a person's belongings is not permitted." United States v. Cook, 657 F.2d 730, 733 (5th Cir. Unit A 1981).[10] "The fact that [a] warrant call[s] for seizure of a broad array of items does not, in and of itself, prove that the warrant fails to meet this requirement of particularity." United States v. Sugar, 606 F. Supp. 1134, 1151 (S.D.N.Y. 1985). See also United States v. Ninety-Two Thousand Four Hundred

[10] Decisions of the Fifth Circuit rendered before October 1, 1981, are binding precedent in the Eleventh Circuit. Bonner v. City of Prichard, 661 F.2d 1206, 1209 (11th Cir. 1981) (en banc).

Twenty-Two Dollars and Fifty-Seven Cents, 307 F.3d 137, 149 (3d Cir. 2002) ("Although the scope of the warrant was certainly extensive, the warrant was not general."). "The warrant must enable the searcher to reasonably ascertain and identify the things which are authorized to be seized." Cook, 657 F.2d at 733 (citations omitted). See also Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971). Furthermore, under Federal Rule of Criminal Procedure 41(e)(2)(B), a warrant "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information," and "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." Fed. R. Crim. P. 41(e)(2)(B).

The warrants in this case were not general warrants because they described with sufficient particularity not only the information to be disclosed from Lee's Gmail accounts, but also the specific evidence which the government was allowed to seize from within that body of information. That is, while Attachment A of the warrants required Google to disclose the entire contents of the accounts, Attachment B limited the items authorized to be seized by the government to evidence reasonably connected to the crime of copyright infringement based upon the indicia of probable cause in the affidavits. The warrants thus properly constrained the discretion of the executing agents and enabled them to reasonably ascertain and

identify the limited information which was authorized to be seized. Because the warrants authorized the searching agents to review the information obtained from Lee's Gmail accounts only for evidence relevant to the government's investigation of the crime of copyright infringement, and not for evidence of general criminal activity or evidence otherwise defined by some open-ended criteria that would permit a free-range seizure of information from Google's disclosure, they did not allow a "general, exploratory rummaging" in violation of the Fourth Amendment's particularity requirement, and Lee's argument in this regard is without merit. See United States v. Maharaj, No. 07-80024-CR-CR, 2007 WL 2254559, at *11 (S.D. Fla. Aug. 2, 2007), adopted at *1 (quoting United States v. Wuagneux, 683 F.2d 1343, 1348-49 (11th Cir. 1982)).

Indeed, the two-step procedure employed by the government to review the email accounts in this case—first obtaining the disclosure from Google and subsequently reviewing the disclosure for the items specified in the warrants—is explicitly authorized by Rule 41 of the Federal Rules of Criminal Procedure, and federal courts around the country have consistently upheld similar email search warrants utilizing this same procedure as constitutional under the Fourth Amendment. See United States v. Tsarnaev, 53 F. Supp. 3d 450, 458 (D. Mass. 2014); In the Matter of Search of Info. Associated with [redacted]@mac.com that is Stored

at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157, 165–66 (D.D.C. 2014); In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc., 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014) (collecting cases) ("Notably, every case of which we are aware that has entertained a suppression motion relating to the search of an email account has upheld the Government's ability to obtain the entire contents of the email account to determine which particular emails come within the search warrant."); United States v. Lustyik, No. 2:12-CR-645-TC, 2014 WL 1494019, at *7 (D. Utah Apr. 16, 2014) (citations omitted) (language in warrants which limited the evidence investigators could seize "was more than sufficient to limit the scope of the warrants, and prevent[ed] the warrants from being generalized warrants"); United States v. Deppish, 994 F. Supp. 2d 1211, 1219–21 (D. Kan. 2014) (search warrant appropriately required email service provider to disclose the entire contents of email account, where the warrant further limited the information to be seized from those contents to evidence of a particular crime); United States v. Taylor, 764 F. Supp. 2d 230, 237 (D. Me. 2011) (footnote omitted) ("The Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider

or to ascertain which [pieces of online information] are relevant before copies are obtained from the internet service provider for subsequent searching.").[11]

To the extent Lee argues that the warrants were not sufficiently particularized because they lacked a temporal limitation on the information to be disclosed from the accounts, see [Doc. 54 at 7–14 (arguing in part that the warrants were general warrants because they included no temporal limitations on the information sought)], the Court finds that the warrants were already adequately particularized based on the subject matter limitation to evidence relating to criminal copyright infringement, and therefore an additional temporal limitation was not required. Moreover, as the government points out, the agents had "good reason not to include a temporal limitation in the warrants," since they did not know, when they obtained the warrants, whether Applanet existed in some other form at the time the accounts were first opened in 2004, and since, even assuming certain emails predated the alleged onset of the criminal activity forming the basis of the warrant applications,

---

[11] See also Andresen v. Maryland, 427 U.S. 463, 482 (1976) (noting that, even "[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized"); In the Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d at 166 (explaining that "the practical realities of searches for electronic records may require the government to examine information outside the scope of the search warrant to determine whether specific information is relevant to the criminal investigation and falls within the scope of the warrant").

those emails might nevertheless prove relevant to determining the identity of the defendants involved and the ownership of the accounts in question, which could be important for authenticating the evidence and laying a proper foundation. See [Doc. 71 at 11-13]; see also United States v. Intakanok, No. CR 114-060, 2014 WL 4825368, at *8 (S.D. Ga. Sept. 25, 2014) (finding that "warrants were properly limited to searching the email account . . . for specific categories of information that bear an obvious relationship to the crime alleged," including "information concerning ownership and user identification for the email account"); In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc., 33 F. Supp. 3d at 399. Accordingly, the warrants meet the particularity requirement of the Fourth Amendment, and any evidence seized pursuant to the warrants is not due to be suppressed on the basis that the warrants were unconstitutionally overbroad.

The government further argues that the information sought in paragraphs D and E of Attachment A of the warrants is not subject to suppression because those paragraphs seek only basic subscriber information in which Lee does not have a reasonable expectation of privacy. [Doc. 71 at 14–17]. Lee does not deny that he lacks standing to challenge the seizure of evidence described in paragraphs D and E of Attachment A, but he asserts, without citing to any supporting authority, that

the government has waived this argument by failing to raise it before or during the evidentiary hearing. [Doc. 78 at 8–9]. The government has not waived this argument, however, as it raised it in its initial response to Lee's motion to suppress, [Doc. 71], which was its first substantive briefing on the matter. Cf. In re Egidi, 571 F.3d 1156, 1163 (11th Cir. 2009) (citations omitted) ("Arguments not properly presented in a party's initial brief or raised for the first time in the reply brief are deemed waived."). Moreover, "[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation." United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (collecting cases); see also Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (citations omitted) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); United States v. Christie, 624 F.3d 558, 573 (3d Cir. 2010) (citation omitted) (collecting cases) ("Federal courts have uniformly held that 'subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation' because it is voluntarily conveyed to third parties."); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) ("[Defendant] can point to no evidence that he had a subjective expectation of privacy in his internet and phone 'subscriber information'—*i.e.*, his name, email address, telephone number, and

physical address[.]"); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) ("[E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (collecting cases) (noting that "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator"). Therefore, Lee has no reasonable expectation of privacy in the information described in paragraphs D and E of Attachment A of the warrants, and the suppression of any evidence seized pursuant to those paragraphs is thus unwarranted for this additional reason.

Finally, even if Lee were correct that the warrants were unconstitutionally overbroad, the agents who executed the warrants reasonably relied on their validity, and therefore, evidence seized pursuant to the warrants is not subject to the exclusionary rule. See Leon, 468 U.S. at 926; United States v. Martin, 297 F.3d 1308, 1313–17 (11th Cir. 2002) (good faith exception applied where "the affidavit contained sufficient indicia of probable cause to enable a reasonable officer to execute the warrant thinking it valid" and where the issuing judge "did not cross the line and

wholly abandon his judicial role"); United States v. Taxacher, 902 F.2d 867, 871-72 (11th Cir. 1990) (explaining the limited circumstances in which the Leon good faith exception does not apply); United States v. Maxwell, 920 F.2d 1028, 1034 (D.C. Cir. 1990) (citing Leon, 468 U.S. at 920-21; Massachusetts v. Sheppard, 468 U.S. 981, 987-88 (1984)) (noting that under Leon, "the exclusionary rule should not be applied to exclude evidence seized pursuant to a defective search warrant if the officers conducting the search acted in 'objectively reasonable reliance' on the warrant and the warrant was issued by a detached and neutral magistrate"). Lee argues that the good faith doctrine does not apply because the government executed the warrants without regard to the warrants' terms, and therefore cannot be said to have acted in reasonable reliance on the warrants. [Doc. 78 at 15–16]. Regardless of the alleged deficiencies in the government's execution of the warrants, however, the warrants themselves were clearly not so facially deficient as to preclude an objectively reasonable reliance on their validity, and, for this additional reason, any evidence seized pursuant to the warrants is not due to be suppressed on the basis that the warrants themselves were invalid. See Tsarnaev, 53 F. Supp. 3d at 458; Lustyik, 2014 WL 1494019, at *9–10 (good faith doctrine applied where officers reasonably could have concluded that email warrants were not overly broad since the warrants limited subsequent seizure to information related to specific crimes).

2. Blanket Suppression of the Evidence Seized Pursuant to the Warrants is not Appropriate Based on the Manner in which the Warrants were Executed

Lee next argues that the warrants were executed in a constitutionally flawed manner because the government never determined what evidence from the disclosure provided by Google falls within the scope of the warrants. [Doc. 54 at 14–17; Doc. 78 at 12–15]. As a result, Lee asserts that the government "flagrantly disregarded" the warrants' terms, such that blanket suppression of any evidence seized pursuant to the warrants is an appropriate remedy. [Doc. 54 at 14–17]. The government responds that the warrants were executed in a reasonable manner because Agent Orkin's review of Google's production was limited to a search for information that fell within the scope of the warrants. [Doc. 71 at 20–23].

"'Absent a flagrant disregard of the terms of the warrant, the seizure of items outside the scope of a warrant will not affect admissibility of items properly seized,'" and "total suppression of all items seized 'is not appropriate unless the executing officers' conduct exceeded any reasonable interpretation of the warrant's provisions.'" United States v. Hill, No. CR 114-028, 2014 WL 5410214, at *8 (S.D. Ga. Oct. 23, 2014) (quoting United States v. Khanani, 502 F.3d 1281, 1289 (11th Cir. 2007)). "Nor does the use of officer discretion in reviewing items before deciding whether to seize them amount to flagrant disregard of the terms of the warrant,"

since "[t]he practical realities of a search permit a brief perusal of items to determine what is authorized by a warrant." Id. (citations omitted) (citing United States v. Miranda, 325 F. App'x 858, 860 (11th Cir. 2009) (per curiam) (unpublished)). Indeed, "[t]he extreme remedy of blanket suppression should only be imposed in the most 'extraordinary' of cases.'" United States v. Brooks, No. 3:13-cr-58-J-34JRK, 2014 WL 292194, at *15 (M.D. Fla. Jan. 27, 2014) (alteration in original) (quoting United States v. Foster, 100 F.3d 846, 852 (10th Cir. 1996))).

The record in this case establishes that Agent Orkin limited his review of Google's production to a search for evidence related to the particular crimes specified in the warrants, and the government's execution of the warrants was therefore not unreasonable under the Fourth Amendment. There is nothing to suggest that Agent Orkin somehow exceeded the scope of the warrants by conducting an indiscriminate search of the records for general criminal activity. On the contrary, Agent Orkin testified that he "went through the e-mails and determined if they related to this investigation or the affidavit"; sorted the emails into subfolders according to their "relevancy to the investigation"; and then selected certain emails that "were of importance in the investigation[.]" (Tr. at 8–9, 18, 21–22); see also (Tr. at 25 (confirming that the information he sought from the investigation was simply what was encompassed in the warrant affidavits)). Based

on the credible testimony presented at the evidentiary hearing, the Court finds that Agent Orkin's review of the records produced by Google consisted of looking for information directly related to the alleged violations of copyright law described in the warrants. In sum, because Agent Orkin's search of the emails was tailored to retrieve information responsive to the warrants, the search did not amount to a general rummaging in flagrant disregard for the warrants' limitations, and blanket suppression of the evidence seized pursuant to the warrants is not appropriate. See Brooks, 2014 WL 292194, at *12 (citations omitted) (finding no flagrant disregard of the warrant where the search was carried out in a "controlled manner" based on the warrant's limitations).[12]

At the same time, however, it is clear from Agent Orkin's testimony that, at the time of the hearing, the government had not completed reviewing the records

[12] That the government's discovery disclosure to Lee consisted of the entire contents of Google's production, including those emails that were not responsive to the warrants, does not suggest that the warrants were improperly executed. See [Doc. 54 at 10]; (Tr. at 23–24). The government's review of the emails and its disclosure of the emails in discovery are two separate matters, and there is no evidence from which to infer that the scope of the government's search of the emails bore any relation to the scope of its discovery disclosure. See Lustyik, 2014 WL 1494019, at *14 (rejecting defendants' argument that the government's discovery disclosure of all emails obtained pursuant to search warrants was evidence that the warrants were improperly executed; that the government "properly took an expansive view of what to produce in discovery" did not undermine the controls undertaken by the government to review the emails only for information that fell within the scope of the warrants).

produced by Google for seizure of the information described in Attachment B of the warrants. There is some disagreement as to precisely what it means to "seize" electronic information under the two-step procedure of Federal Rule of Criminal Procedure 41—where the government first obtains a collection of information, then searches it consistent with the warrant, and finally seizes what is authorized by the warrant from the information already obtained. But it is not necessary to define the contours of what constitutes a seizure in this context in order to conclude that the government has not completed the seizure of information authorized by the warrants in this case. Where, as here, the government has in its possession a production of electronic data that includes a subset of information within the scope of the warrant by which the production was obtained, the seizure of the information authorized by the warrant must, at a minimum, entail a reasonably definite segregation of the data that is subject to seizure from that which is not. See United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) (per curiam) (describing the seizure of electronic records as "[t]he process of segregating electronic data that is seizable from that which is not"). Although Agent Orkin searched the records produced by Google for information he was authorized to seize, triaged that information for relevancy to the investigation, and selected certain items of information to be communicated to others, it does not appear that, at least

at the time of the evidentiary hearing, he had segregated the emails responsive to the warrants from those which admittedly bore no relation to the investigation.[13]

As mentioned earlier, Agent Orkin testified that he would typically organize information obtained from an electronic search into "subfolders that [he] created so that [he] could go back and read through them." (Tr. at 8). Thus, Agent Orkin appears to have used the subfolders to categorize certain pieces of information found within an electronic production, but notwithstanding his testimony about the subfolders, Agent Orkin indicated that the emails responsive to the warrants remain stored together with the emails that were unrelated to the investigation. See (Tr. at 23); [Doc. 71 at 5 (government conceding that Agent Orkin "stated that the emails that are not related to the investigation remain stored with the emails relevant to the investigation")]. And while Agent Orkin also confirmed that he "select[ed]" certain unidentified emails "for future use" in the investigation, he did not indicate that the selected emails were in any way segregated from those that were not selected, or that the "selections" were made specifically to identify the emails authorized to be

[13] Lee asserts that, contrary to the record and representations made at the evidentiary hearing, the government's post-hearing brief erroneously states that Agent Orkin "received the production from Google and reviewed it to determine what fell within the scope of the warrant." [Doc. 78 at 2 (citations and internal marks omitted)]. However, the government's surreply clears up any confusion on this point, and the Court is fully satisfied that the government did not attempt to mislead the Court at the hearing or in its brief.

seized. (Tr. at 9–10). However, Agent Orkin's procedures, though perhaps incomplete, were not inconsistent with the terms of the warrant or the procedure described in the affidavits in support of the search warrant applications because neither put a time limit on completing the seizure.

Rule 41(e)(2)(B) specifically authorizes "the seizure of electronic storage media or the seizure or copying of electronically stored information," and "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." Fed. R. Crim P. 41(e)(2)(B). The rule further provides that the time for executing such a warrant "refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." Id. Consistent with Rule 41, the warrants here did not place a time limit on the off-site copying and review of the records obtained pursuant to the warrant. The warrants were executed by service upon Google, which then produced the records in Attachment A, and Attachment B specified the items to be seized from the records produced by Google. [Doc. 54-1 at 23, 49]. The affidavit in support of the search warrant applications specified that "[u]pon receipt of the information described in Attachment A, the information described in Attachment B, which includes any evidence, fruits, and instrumentalities of violations of 17 U.S.C. § 506 and 18 U.S.C. § 2319 (infringement of a copyright), will be subject to seizure by law

enforcement." [Doc. 54-1 at 13, 39]. Thus, although the government has not completed the review and seizure of all records authorized by the warrants, it has not violated the terms of the warrants by not doing so.[14] By merely failing to seize all responsive information from Google's production, the government has not flagrantly disregarded the terms of the warrants in a way that would justify the extreme remedy of blanket suppression of the evidence.[15]

---

[14] The government, of course, is not obligated to locate and seize all of the information that is authorized by the warrants; however, for any records that the government does intend to seize, it shall segregate those records from the remainder of the Google production and provide Lee a copy of those seized records. Absent segregation and identification of the records seized, there is no basis for discerning whether particular records were seized consistent with the terms of the warrant.

[15] Lee also argues that the amount of time that the government has retained the entire production of Lee's Gmail accounts is constitutionally impermissible. [Doc. 78 at 13–15]. Lee suggests that, after its initial review of the emails, the government was required to return or destroy any emails that it determined fell outside of the scope of the warrants. [Id. at 13–15]. There is no requirement, however, either in the warrants or in the Constitution, that the government return or destroy lawfully obtained evidence relevant to an ongoing criminal investigation while the criminal proceedings related to that investigation remain pending. Indeed, "[t]he general rule is that lawfully seized property bearing evidence relevant to trial should be returned to its rightful owner once the criminal proceedings have terminated, not before," and Lee "offers no reason to think [his] case an exception to this general rule." Christie, 717 F.3d at 1167 (citations and internal marks omitted). The government's search and seizure of information within the production obtained pursuant to the warrants is not incompatible with the temporary or conditional retention of the remaining production, which may be necessary for authentication, as well as establishing Lee's identity and his alleged ownership of the accounts. Accordingly, the Court finds no constitutional infirmity in the government's retention of Google's production while these proceedings remain pending. See In the Matter of Search of Info. Associated with

3. The Warrants were not Obtained in Violation of *Franks*

Lee's final argument in support of suppression is that the warrants were obtained in violation of Franks because the affidavits supporting the warrants omitted several "critical facts[.]" [Doc. 68 at 6–8; Doc. 78 at 11–12]. In particular, Lee contends that when the government applied for the warrants, it knew that the email accounts in question were created in 2004, and that Applanet, the entity under investigation, did not exist between 2004 and 2009. [Doc. 68 at 2, 7; Doc. 78 at 11-12]. As a result, Lee argues, the government knew that "it would not find any evidence

---

[redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d at 167 n.10 (citation and internal marks omitted) (discussing the government's "valid" concerns that destroying or returning the emails received from an online service provider "could either expose the government to accusations that it destroyed exculpatory evidence," or "hinder the government's ability to lay a foundation for evidence and establish authenticity"); In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc., 33 F. Supp. 3d at 399 (noting that "it may be necessary for the Government to maintain a complete copy of the electronic information to authenticate evidence responsive to the warrant for purposes of trial"); Brooks, 2014 WL 292194, at *15 (citation omitted) (rejecting "[d]efendant's argument that that the Government's retention of [] non-contraband items . . . justifies suppression of lawfully-seized evidence"). Thus, the Court declines to impose a deadline on the government's retention of the Google production while the case remains pending, and Lee has other remedies available short of blanket suppression of the evidence seized pursuant to the warrants should he contend that the government has improperly retained the records. See In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc., 33 F. Supp. 3d at 398 (noting other remedies available if the government retains a "copy of emails beyond a constitutionally reasonable period").

even remotely related to this investigation in [] Lee's emails" from from 2004 through 2009, yet the government nevertheless sought to obtain the entire contents of Lee's email accounts, which included information from those years. [Doc 68 at 7; Doc. 78 at 11]. Essentially, then, Lee maintains that the government violated Franks by "failing to tell the Court that it had no evidence to support its request for [] Lee's emails for the years" of 2004 through 2009. [Doc. 68 at 2]. The government counters that the warrants were not obtained in violation of Franks because Lee has failed to show either that any omissions in the applications were knowing or reckless, or that any of the omitted facts, if included, would have prevented a finding of probable cause. [Doc. 71 at 18–20].

A presumption of validity attaches to an affidavit supporting a search warrant application. Franks, 438 U.S. at 171. "Under *Franks*, a defendant may attack a facially sufficient affidavit supporting a search warrant if (1) it contains statements or omissions that were deliberately false or demonstrated a reckless disregard for the truth and (2) those challenged statements or omissions are essential to the magistrate judge's finding of probable cause." United States v. Bell, 692 F. Supp. 2d 606, 610 (W.D. Va. 2010) (citations omitted). See also Maharaj, 2007 WL 2254559, at *6; United States v. Burston, 159 F.3d 1328, 1333 (11th Cir. 1998). "'The *Franks* standard is a high one.'" United States v. Nakouzi, No. 3:05CR154(MRK), 2005 WL

3211208, at *5 (D. Conn. Nov. 30, 2005) (quoting Rivera v. United States, 928 F.2d 592, 604 (2d Cir. 1991)).

Negligent or innocent mistakes in a warrant application do not violate a defendant's Fourth Amendment rights. See Maughon v. Bibb Cnty., 160 F.3d 658, 660 (11th Cir. 1998) (per curiam); Madiwale v. Savaiko, 117 F.3d 1321, 1326-27 (11th Cir. 1997); Franks, 438 U.S. at 171. Moreover, "'[i]nsignificant and immaterial misrepresentations or omissions will not invalidate a warrant.'" Maharaj, 2007 WL 2254559, at *7 (quoting United States v. Ofshe, 817 F.2d 1508, 1513 (11th Cir. 1987)). Indeed, every fact recited in an affidavit in support of an application for a search warrant does not necessarily have to be correct, but the affidavit must be truthful in the sense that it is believed or appropriately accepted by the affiant as true. Franks, 438 U.S. at 165.

Lee also bears the burden of showing that absent the alleged misrepresentations or omissions, probable cause would have been lacking. United States v. Umole, 162 F. App'x 948, 950 (11th Cir. 2006) (per curiam) (unpublished) (citation omitted) (quoting United States v. Novaton, 271 F.3d 968, 987 (11th Cir. 2001)). However, "if the court is satisfied that when material that is the subject of the alleged falsity or reckless disregard is set to one side[(or, in the case of an omission, when the omitted material is included)], there remains sufficient content

in the warrant affidavit to support a finding of probable cause, then no hearing is required." Nakouzi, 2005 WL 3211208, at *5 (internal citation and marks omitted).

It is undisputed that the government knew, at the time the affidavits in support of the search warrant applications were presented to the Court, that the email accounts at issue were created in 2004. See (Tr. at 12–13, 16). The government also acknowledges that Agent Orkin "knew that Applanet could not have existed in its current form in 2004, as the Android operating system was not created until 2007, but he did not know whether Applanet existed in any form in 2004." [Doc. 71 at 5-6]. Agent Orkin clearly testified that, at the time the government sought the search warrants, the agents "did not know" whether Applanet existed in some form in 2004. (Tr. at 17 ("Q. Well, did [Applanet] exist in any form in 2004? A. At this point in the investigation we did not know.")). Lee attempts to rebut this testimony by pointing to Agent Orkin's related statement that "Applanet did not" exist from the years 2004 through 2009. See [Doc. 78 at 11 (quoting (Tr. at 17))]. Agent Orkin made this statement, however, in response to a straightforward question by defense counsel as to whether Applanet existed from 2004 through 2009. Because the government did not know, when it presented the affidavits, whether Applanet might have existed in some other form as early as 2004, the affiant did not make any material omission of information in the affidavit in support of the search warrant

applications as he had no reason to believe that emails between 2004 and 2009 would not be relevant to the investigation.

Lee further argues that, regardless of whether the government knew if Applanet existed in some form in 2004, it was still impermissible for the government to seek any emails prior to 2007, since that is the year the Android operating system was created, and the investigation focused on copyright infringement related to that particular operating system. [Doc. 78 at 12]. As previously discussed, however, there were legitimate reasons for the government to include in the search warrant applications a request for emails that may have predated the onset of the criminal activity to which the account was allegedly connected, such as authenticating the evidence, establishing identity and ownership, and laying a proper foundation for admission of the records at trial. See [Doc. 71 at 11-13]; Intakanok, 2014 WL 4825368, at *8; In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc., 33 F. Supp. 3d at 399.

Moreover, even if the government had included in the affidavits the fact that the email accounts in question were opened in 2004—which is the only omitted fact identified by Lee of which the government was actually aware at the time it sought the warrants—the inclusion of that fact would not have prevented a finding of

probable cause, since, as the Court has already discussed, the government did not know at that time whether Applanet existed in some form as early as 2004. See Maharaj, 2007 WL 2254559, at *6 (citation omitted) (noting that "'immaterial . . . omissions will not invalidate a warrant'"). Nor is there any question that the affidavits otherwise presented a sufficient factual basis to support a finding of probable cause to search the accounts consistent with the limitations set forth in the warrants. For instance, the affidavits indicate that Applanet was "actively sharing copyrighted works for free," [Doc. 54-1 at 9 ¶ 18, 35 ¶ 18]; that the administrators of Applanet acknowledged on their website that they knew that what they were doing was illegal, [id. at 9 ¶ 20, 35 ¶ 20]; that the Applanet website included a link to an administrative protocol panel, which listed the name "The Buzzer" as the "unofficial coder," with a contact email address of thebuzzer@gmail.com, [id. at 10 ¶ 22, 36 ¶ 22]; that "The Buzzer" posted a message on the Applanet website explaining how to "'[b]ypass google license [sic] check a easy way,'" [id. at 10 ¶ 23, 36 ¶ 23 (second alteration in original)]; that emails sent from the flyingbuzz@gmail.com to a co-conspirator provided source code corresponding to an Android application that was being distributed by Applanet in order to provide access to copyrighted commercial works free of charge, [id. at 11 ¶ 26, 37 ¶ 26]; and that a subpoena issued to Google revealed that the flyingbuzz@gmail.com was a secondary email address associated

with the primary email account of thebuzzer@gmail.com, [id. at 11 ¶ 25, 37 ¶ 25]. The affidavits thus establish probable cause to search the two email accounts regardless of whether the accounts were created in 2004 or at some later time. Accordingly, the warrants were not obtained in violation of Franks, and Lee's motion to suppress any evidence obtained pursuant to the warrants is due to be denied.

III. CONCLUSION

For the foregoing reasons, the government's motion for leave to file a surreply, [Doc. 80], is **GRANTED**, and the Clerk is **DIRECTED** to enter the government's surreply, [Doc. 80-1], on the docket. Lee's "Motion to Require the Government to Remove Portions of an Offending Press Release from All DOJ Websites," [Doc. 53], is **DENIED**, and it is **RECOMMENDED** that Lee's motion to suppress evidence, [Doc. 54], be **DENIED**.

There are no other pending matters before the Magistrate Judge, and the undersigned is aware of no problems relating to the scheduling of this case.

IT IS THEREFORE ORDERED and **ADJUDGED** that this action be and the same is hereby, certified Ready for Trial.

IT IS SO ORDERED AND RECOMMENDED, this 6th day of July, 2015.

Russell G. Vineyard

RUSSELL G. VINEYARD
UNITED STATES MAGISTRATE JUDGE